Internal Audit Report

Computer Virus Detection Controls

January 2001

Audit Team Members

Sandy Chockey, IS Audit Manager

Susan Adams, Senior IS Auditor

Deloitte & Touche, LLP

Internal Audit Department

301 W Jefferson • 10th Floor • Phx • AZ • 85003 • (602) 506-1585 • Fax (602) 506-8957

January 5, 2001

Janice K. Brewer, Chairman, Board of Supervisors
Fulton Brock, Supervisor, District I
Don Stapley, Supervisor, District II
Andrew Kunasek, Supervisor, District III
Mary Rose Wilcox, Supervisor, District V

We have completed our FY 2001 review of the County's Computer Virus Detection Controls. The audit was performed in accordance with the annual audit plan approved by the Board of Supervisors. In addition to reviewing the County's overall policies and procedures, we examined virus detection controls within five major County organizations: County Attorney's Office, Sheriff's Office, Department of Human Services, Superior Court, and Maricopa Integrated Health System (MIHS).

Overall, we found that County management effectively administers computer virus detection controls. We also identified areas needing improvement. These, along with our recommendations, are detailed in the attached report. Highlights include:

- A countywide virus detection policy is being developed but has not been finalized and communicated to County departments. Many departments do not have specific anti-virus procedures related to the department's operations.
- System users have the ability to modify or disable virus detection software from their workstations.
- Virus detection software has not been installed on some servers that support major business operations.

Attached are the individual audit reports and responses from the respective County and Superior Court officials. We have reviewed the details of this work with the management of each organization and appreciate the cooperation received during the review. If you have questions, or wish to discuss items presented in this report, please contact Sandy Chockey at 506-1006.

Sincerely,

Ross L. Tate

Ross L. Tate
County Auditor

Table of Contents

Executive Summary

Office of the Chief Information Officer (Page 5)

The Office of the CIO has not finalized its policies related to virus protection. Departments and users cannot be held accountable if policies and procedures have not been developed or formally approved and distributed by management. The Office of the CIO should enhance, finalize, and communicate a comprehensive virus protection policy, which will provide a standard to all County departments.

Electronic Business Center (Page 7)

The Electronic Business Center (EBC), under the direction of the Office of the CIO, has not developed a comprehensive set of policies and procedures relating to virus protection for the County's Exchange mail servers. The lack of adequate policies and procedures increases the risk that a virus can be introduced into the environment. EBC should develop departmental virus protection policies and procedures.

Human Services Department (Page 9)

The Human Services Department (HSD) has not installed virus protection software on its servers and has not developed a comprehensive set of policies and procedures relating to virus protection. These control weaknesses increase the risk that viruses can be spread throughout the department and the County. HSD should strengthen its virus protection controls.

Superior Court (Page 11)

The Superior Court has not installed virus protection software on its

web servers or Winframe servers. Superior Court system users have the ability to modify, remove, or disable the installed anti-virus software, which increases the risk that viruses can be introduced into the environment and spread through the court system and the County. The Superior Court should strengthen its virus protection.

County Attorney (Page 13)

The Maricopa County Attorney's Office (MCAO) system users have the ability to modify, remove, or disable the installed anti-virus software from their workstations. Inadequate virus protection controls increase the risk that a virus can be introduced into the environment. MCAO should strengthen its virus protection controls.

Sheriff's Office (Page 14)

The Maricopa County Sheriff's Office (MCSO) has established guidelines relating to virus protection, however, system users have the ability to modify, remove, or disable the installed anti-virus software. The control weakness increases the risk that a virus can be introduced into the environment. MCSO should strengthen its virus detection controls by limiting user access to the anti-virus software and enhancing virus protection guidelines.

Maricopa Integrated Health Systems (Page 15)

Maricopa Integrated Health Systems (MIHS) users have the ability to modify, remove, or disable the installed anti-virus software. MIHS has not developed a comprehensive set of policies and procedures related to virus protection. The lack of adequate virus protection controls may allow an undetected virus to enter the MIHS system and possibly infect other County systems. MIHS should implement sound virus protection controls.

Introduction

Background

Computer viruses are increasing at an unprecedented rate. Only one virus was identified in 1986 and three years later, the number had increased to six. The total jumped to 80 by 1990 and by November 1990, viruses were being discovered at a rate of one per week. Today, 10 to 15 new viruses appear every day. Industry estimates are that between December 1998 to October 1999, the total virus count rose from 20,500 to 42,000.

Computer viruses spread by attaching themselves to another program (e.g., word processing, spreadsheet, etc.) or to the boot sector of a diskette. When an infected file is executed, or the computer is started from an infected disk, the virus itself is executed. The virus often stays in memory, waiting to infect the next program that is run or the next disk that is accessed. Many viruses perform trigger events. For example, they might display a message on a certain date or delete files after the infected program is run a certain number of times. While some trigger events are benign, others can be very costly and cause significant damage.

According to the International Computer Security Association (ICSA), the financial cost of virus infection, measured in cost per incident, averaged $2,454 in 1998. The 1998 study also reports that complete recovery from an infection requires an average of 45.6 hours and 9.4 person-days of work. Often the cost is much more; one study respondent reported a cost of $150,000 for a single incident. The ICSA study concluded that reported virus infection costs would be much higher if related costs, such as loss of business and lower productivity, were taken into consideration.

More recently, the Yankee Group in Boston estimated that the denial of service attacks, instigated by a virus, has cost the e-commerce industry 1.2 billion dollars. For this reason and others, our office initiated a review of the County's anti-virus readiness.

Industry Best Practices

Industry best practices are to scan all incoming and outgoing files with the most current anti-virus software and virus definitions on all firewalls, file servers, application servers, and workstations in the environment. Virus protection software should be incorporated into the firewall to detect and prevent viruses from infecting and destroying computer data before the virus enters the

environment. Furthermore, current virus protection software should be loaded on all file servers and workstations within the environment to protect against any virus that may penetrate the system.

Additionally, a procedure should be implemented that would require the most recent virus definition to be placed on all machines with virus protection software. Nearly 1,000 new viruses are being created monthly and new virus definitions are being developed weekly by most anti-virus software providers. New virus definitions are critical to defend against viruses. Some new virus definitions will require virus protection software to be updated. Therefore, the newest anti-virus software should be loaded in addition to the new virus definitions.

Once the most recent version of anti-virus software has been loaded onto all machines within the environment, these must be scheduled to scan for viruses. To prevent virus attacks from infecting an environment, best practices have shown that all incoming disks, files, executables, and e-mail attachments that enter an environment should be scanned before opened on a workstation or server. Even with this precautionary procedure, the risk is still present that a new virus (not part of the virus definition) could be created and penetrate the environment prior to loading the definition to combat that virus. Therefore, the virus software should be scheduled to regularly scan all drives on the machine to detect such viruses.

Scope and Methodology

Our audit objectives were to determine if:

- The County has developed and implemented policies and procedures that accurately reflect the intentions of management and lend themselves to thorough protection from virus infections.
- Information housed on the network is safeguarded against viruses by current virus protection software.
- Virus protection is comprehensive and is maintained on all of the appropriate equipment.
- Virus protection software is scheduled to scan on an appropriate schedule that would lead to sound virus protection.

This audit was performed in accordance with Government Auditing Standards.

Office of the Chief Information Officer (CIO)

Summary

The Office of the CIO has not finalized its policies related to virus protection. Departments and users cannot be held accountable if policies and procedures have not been developed or formally approved and distributed by management. The Office of the CIO should enhance, finalize, and communicate a comprehensive virus protection policy, which will provide a standard to all County departments.

Applicable Requirements

County Policy A1601 states that the "CIO is responsible for managing the governance structure including…establishing security principles and guidelines…" Adequate computer virus detection control policies and procedures are an integral part of security principles developed to protect information assets.

Enterprise-wide Policy

The Office of the CIO has made a concerted effort to strengthen virus protection controls within the County. We reviewed the County's enterprise-wide virus protection controls and noted the following:

- Policies and procedures related to virus protection have been drafted but have not been finalized or formally adopted. Departments and users cannot be held accountable if policies and procedures have either not been developed or have not been formally approved and distributed by management.
- The County has not prescribed specific preventive and detective controls that should be put in place at the department level to ensure adequate and thorough coverage against virus infection. Without identifying and addressing these controls, the County does not have assurance that its current method of addressing virus protection is adequate or thorough.
- A wide difference exists in how each department addresses virus protection and how actual virus protection software has been enabled (e.g., scanning all versus some files, daily versus weekly scans, installing virus software on all versus select servers). Without a baseline standard for all departments to follow, the County increases the risk of inadequate virus protection administration and inappropriate settings within the software.

Recommendations

The Office of the CIO should:

A. Finalize its draft policies and procedures, in a timely manner, to ensure that the County's virus protection position is communicated to all departments.

B. Perform follow-up activities, once the final policies and procedures have been approved, to ensure adherence by all County departments.

C. Enhance the currently drafted policies and procedures to identify and detail specific preventive and detective controls that should be put into place at the department level.

D. Develop a minimum baseline standard relative to how virus protection is both administered and enabled. These standards should be developed to allow departments certain flexibility, but also be specific enough to set the overall "tone" for how the County will address virus protection.

See Department Response on page 20.

Electronic Business Center

Summary

The Electronic Business Center (EBC), under the direction of the Office of the CIO, has not developed a comprehensive set of policies and procedures relating to virus protection for the County's Exchange mail servers. The lack of adequate policies and procedures increases the risk that a virus can be introduced into the environment. EBC should develop departmental virus protection policies and procedures.

Applicable Requirements

County policy A1601 states that "the Technology Officer at each level of the organization is responsible for protecting information assets against deliberate attack or sabotage, and unintentional or unauthorized alteration, destruction, or disclosure." Adequate computer virus detection control polices and procedures are an integral protection component against such harm.

EBC Virus Protection

EBC appears to be taking proper steps to ensure adequate virus detection over the County's Exchange mail servers. However, the office has not developed a complete set of policies and procedures relating to virus protection. This control is necessary to ensure a comprehensive knowledge transfer in the absence of employees that perform the day-to-day operations, relating to viruses.

The absence of adequate policies and procedures increases the likelihood of activity occurring that is inconsistent with management's intentions. Additionally, the office faces increased risk that new employees will not be able to take over the responsibilities without incident.

Recommendations

EBC should develop specific and detailed virus protection policies and procedures that accurately reflect management's intentions and provide a level of detail that allows for any competent person to fulfill the responsibilities.

See Department Response on page 23.

--Blank Page--

Human Services Department

Summary

The Human Services Department (HSD) has not installed virus protection software on its servers and has not developed a comprehensive set of policies and procedures relating to virus protection. These control weaknesses increase the risk that viruses can be spread throughout the department and the County. HSD should strengthen its virus protection controls.

Applicable Requirements

County policy A1601 states "… the Technology Officer at each level of the organization is responsible for protecting information assets against deliberate attack or sabotage, and unintentional or unauthorized alteration, destruction, or disclosure." Adequate computer virus detection control polices and procedures are an integral protection component against such harm.

HSD Virus Protection - Servers

Anti-virus software has not been installed on any servers within HSD. Although the servers do not have a lot of file movement, they support some of HSD's most critical network applications. If these machines were infected, major operational inefficiencies could occur. We understand that each server is manually scanned 2 to 4 times each week for viruses. Formalized procedures for these manual scans have not been developed nor has a log been created to ensure that all servers are manually scanned at least once per week.

If virus detection software is not used to check for viruses on a real time basis, the risk increases that viruses can be spread through the department and County. The lack of formalized procedures increases the likelihood that the servers may not be scanned if the individual responsible for performing the manual scans is on vacation, sick, or has terminated employment. Additionally, the absence of a log showing all servers' scans increases the risk that not all servers are scanned at least weekly.

HSD Virus Protection – Policy and Procedure

HSD has not developed a comprehensive set of policies and procedures related to virus protection. This control is necessary to ensure a comprehensive knowledge transfer, in the absence of employees that perform the day-to-day operations relating to viruses.

The absence of adequate policies and procedures increases the likelihood of activity occurring that is inconsistent with management's intentions. Additionally, the office faces increased risk that new employees will not be able to take over the responsibilities without incident.

Recommendations

HSD should:

A. Install virus protection software at the server level so that all are actively scanning for viruses. This protection will help to ensure that viruses are not allowed to circulate and infect other County servers and workstations.

B. Develop specific and detailed virus protection policies and procedures that accurately reflect management's intentions and provide a level of detail that would allow for any competent person to fulfill the responsibilities.

See Department Response on page 24.

Superior Court

Summary

The Superior Court has not installed virus protection software on its web servers or Winframe servers. Superior Court system users have the ability to modify, remove, or disable the installed anti-virus software, which increases the risk that viruses can be introduced into the environment and spread through the court system and the County. The Superior Court should strengthen its virus protection.

Applicable Requirements

County policy A1601 states "… the Technology Officer at each level of the organization is responsible for protecting information assets against deliberate attack or sabotage, and unintentional or unauthorized alteration, destruction, or disclosure." Adequate computer virus detection control polices and procedures are an integral protection component against such harm.

Superior Court Virus Protection

During our review of the Superior Court's virus protection controls, we made the following observations:

- Anti-virus software has not been installed on the Superior Court web and Winframe servers. We understand, however, that the Winframe servers are to be phased out with Metaframe servers, which are running anti-virus software. The placement of virus detection software on the servers has been discussed but not yet implemented. If the Superior Court does not use virus detection software to check for viruses, on a real time basis, the court increases the risk that viruses can be spread through its system and the County.
- No restrictions have been established to prevent system users from modifying or disabling the workstation virus detection software. In addition, policies and procedures have not been developed to prohibit users from altering or disabling the virus detection software. This control weakness increases the risk that a virus can be introduced into the environment. Unless users are made aware of their responsibilities, the task of holding them accountable for making changes or disabling the virus software is made more difficult.
- The Superior Court has not developed a comprehensive set of policies and procedures related to virus protection. This control is necessary to ensure a comprehensive knowledge transfer, in the absence of employees that perform the day-to-day operations relating to viruses.

Recommendations

The Superior Court should:

A. Install virus detection software on all servers so that all servers are actively scanning for viruses. This control will help to ensure that viruses are not allowed to circulate and infect other County servers and workstations.

B. Consider ways to restrict users from being able to modify or disable the virus detection software. Virus protection policies and procedures should include user responsibilities relating to the virus software (i.e., users should not disable or modify the options within the virus software).

C. Develop specific and detailed virus protection policies and procedures that accurately reflect management's intentions and provide a level of detail that would allow for any competent person to fulfill the responsibilities.

See Response on page 25.

County Attorney's Office

Summary

The Maricopa County Attorney's Office (MCAO) system users have the ability to modify, remove, or disable the installed anti-virus software from their workstations. Inadequate virus protection controls increase the risk that a virus can be introduced into the environment. MCAO should strengthen its virus protection controls.

Applicable Requirements

County policy A1601 states: "…the Technology Officer at each level of the organization is responsible for protecting information assets against deliberate attack or sabotage, and unintentional or unauthorized alteration, destruction, or disclosure." Adequate computer virus detection control polices and procedures are an integral protection component against such harm.

MCAO Virus Protection

No restrictions have been established to prevent users from modifying or disabling the workstation virus detection software. In addition, policies and procedures have not been developed which specifically dictate that users should not alter or disable the virus software. This omission increases the risk that a virus can be introduced into the environment. Unless users are made aware of their responsibilities, the task of holding them accountable for making changes or disabling the virus software is made more difficult.

Recommendation

MCAO should consider ways to restrict system user's ability to modify or disable the virus detection software. In addition, virus protection policies and procedures should include user responsibilities relating to the virus detection software (i.e., users should not disable or modify options within the virus software).

See Response on page 29.

Sheriff's Office

Summary

The Maricopa County Sheriff's Office (MCSO) has established guidelines relating to virus protection, however, system users have the ability to modify, remove, or disable the installed anti-virus software. The control weakness increases the risk that a virus can be introduced into the environment. MCSO should strengthen its virus detection controls by limiting user access to the anti-virus software and enhancing virus protection guidelines.

Applicable Requirements

County policy A1601 states "… the Technology Officer at each level of the organization is responsible for protecting information assets against deliberate attack or sabotage, and unintentional or unauthorized alteration, destruction, or disclosure." Adequate computer virus detection control polices and procedures are an integral protection component against such harm.

MCSO Virus Protection

MCSO has not established restrictions to prevent users from modifying or disabling the workstation virus detection software. MCSO guidelines state, "the personal computer user is solely responsible for insuring that no computer virus is introduced to their system. Virus protection software is loaded on each personal computer and users are responsible for insuring that the software is running when information is assessed." If users are not restricted from modifying or disabling the virus detection software, the risk increases that a virus can be introduced into the environment. Unless users are made aware of their responsibilities, the task of holding them accountable for making changes or disabling the virus software is made more difficult.

Recommendation

MCSO should consider ways to restrict system user's ability to modify or disable the virus detection software. In addition, virus protection policies and procedures should include user responsibilities relating to the virus detection software (i.e., users should not disable or modify options within the virus software).

See Response on page 31.

Maricopa Integrated Health Systems (MIHS)

Summary

Maricopa Integrated Health Systems (MIHS) users have the ability to modify, remove, or disable the installed anti-virus software. MIHS has not developed a comprehensive set of policies and procedures related to virus protection. The lack of adequate virus protection controls may allow an undetected virus to enter the MIHS system and possibly infect other County systems. MIHS should implement sound virus protection controls.

Applicable Requirements

County policy A1601 states "…the Technology Officer at each level of the organization is responsible for protecting information assets against deliberate attack or sabotage, and unintentional or unauthorized alteration, destruction, or disclosure." Adequate computer virus detection control polices and procedures are an integral protection component against such harm.

MIHS Virus Protection

During our review of MIHS's virus protection controls, we made the following observations:

- No restrictions have been put into place that would prevent users from modifying or disabling the installed workstation anti-virus software. Policies and procedures have not been developed which specifically dictate that users should not alter or disable the virus detection software. This control weakness increases the risk that a virus can be introduced into the environment. Unless users are made aware of their responsibilities, the task of holding them accountable for making changes or disabling the virus software is made more difficult.
- MIHS has not developed a comprehensive set of policies and procedures related to virus protection. This control is necessary to ensure a comprehensive knowledge transfer, in the absence of employees that perform the day-to-day operations relating to viruses. The absence of adequate policies and procedures increases the likelihood of activity occurring that is inconsistent with management's intentions. Additionally, the office faces increased risk that new employees will not be able to take over the responsibilities without incident.

Recommendations

MIHS should:

A. Consider ways to restrict users from being able to modify or disable the workstation virus detection software. Virus protection policies and procedures should include user responsibilities relating to the virus detection software (i.e., users should not disable or modify the options within the virus software).

B. Develop specific and detailed virus protection policies and procedures that accurately reflect management's intentions and provide a level of detail that would allow for any competent person to fulfill the responsibilities.

See Department Response on page 32.

--Blank Page--

DEPARTMENT RESPONSES

--Blank Page--